

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
information associated with)
lktechnologies@comcast.net)
)

Case No. 22-1823M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 28, 2022 (not to exceed 14 days)

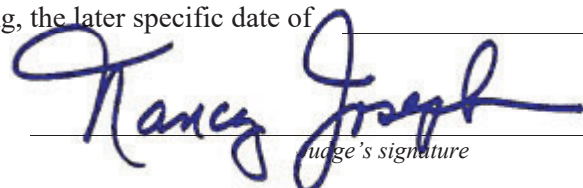
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Nancy Joseph, United States Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11/14/22 @ 6:30 p.m.


Judge's signature

City and state: Milwaukee, Wisconsin

Nancy Joseph, United States Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with lktechnologies@comcast.net, that is stored at premises controlled by Comcast Communications, a company headquartered in Philadelphia, Pennsylvania.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Comcast (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from January 1, 2021 to October 26, 2022:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 DAYS of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Sections 829(e), 841(a)(1), 841(h), 843(c)(2)(A), and 846 and occurring after January 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. The importation and distribution of controlled substances and other prescription medications.
2. Information relating to the identity of any and all individuals who operate or maintain online pharmacies that sell controlled substances and other prescription medications.
3. Records of payment made in relation to the operation and maintenance of online pharmacies that sell controlled substances and other prescription medications, including proceeds from such sales.
4. Information relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.
5. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.
6. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation.
7. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
8. The identity of the person(s) who communicated with the user ID about matters relating to importation and distribution of controlled substances and other prescription medications, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)information associated with
lktechnologies@comcast.net

Case No. 22-1823M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. 829(e), 841(a)(1), 841(h), 843(c)(2)(A), and 846	distribution and possession with intent to distribute a controlled substance, distribution of a controlled substance by means of the Internet, and conspiracy to do the same

The application is based on these facts:

See the attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

SCOTT SIMONS
(Affiliate)
Digitally signed by SCOTT
SIMONS (Affiliate)
Date: 2022.11.10 15:40:05
-06'00'

Applicant's signature

Scott Simons, Task Force Officer (DEA)

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 11/14/22

City and state: Milwaukee, Wisconsin

Nancy Joseph, United States Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANT**

I, Scott Simons, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of application for a search warrant for information associated with a certain account that is stored at premises controlled by Comcast Communications (Comcast), an email provider headquartered in Philadelphia, Pennsylvania. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Comcast to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer assigned to the Milwaukee District Office of the Drug Enforcement Administration (DEA) as a member of the Tactical Diversion Squad (TDS). I specialize in pharmaceutical investigations. I have worked full-time as a federal task force officer for the past 9 years and a full-time law enforcement officer with the Greenfield Police Department for the past 20 years. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

3. During my tenure as a law enforcement officer, I have been involved in the investigation of drug traffickers in Milwaukee County, in the State of Wisconsin, across the United

States, and internationally. I have received training in the investigation of drug trafficking, money laundering, and computer crimes. My training and experience includes the following:

- a. Through informant interviews and extensive debriefings of individuals involved in drug trafficking, I have learned about the manner in which individuals and organizations finance, source, purchase, transport, and distribute controlled substances in Wisconsin, throughout the United States, and internationally.
- b. I have used my training and experience to locate, identify, and seize multiple types of drugs, drug proceeds, and drug contraband.
- c. I have conducted several investigations that have resulted in seizures of criminally derived property, including monetary instruments.
- d. I know that controlled substances, drug paraphernalia, and drug proceeds are sent through the U.S. Postal Service system and other parcel services, such as FedEx and UPS, and I am familiar with many of the methods used by individuals who attempt to use mail services to illegally distribute controlled substances.
- e. I have also relied upon informants to obtain controlled substances from drug traffickers and have made undercover purchases of controlled substances.
- f. I am familiar with the language used over the telephone and other electronic communications to discuss drug trafficking and know that the language is often limited, guarded, and coded. I know the various code names used to describe controlled substances. I also know that drug traffickers often use electronic devices (such as computers and cellular phones), electronic communication services (such as email and messaging applications), and social media to facilitate these crimes.
- g. I know that drug traffickers often register phones, mailboxes, bank accounts, electronic communication services, and other instrumentalities of drug trafficking in the names of others, also known as nominees, to evade law enforcement.
- h. I know that drug traffickers often keep documents and records about the sourcing, ordering, sale, transportation, and distribution of controlled substances.
- i. I know that drug traffickers often use drug proceeds to purchase assets such as vehicles, property, and jewelry. I also know that drug traffickers often

use nominees to purchase or title these assets to avoid scrutiny from law enforcement officials. I know that drug traffickers often secure drug proceeds at locations within their dominion and control, such as their residences, businesses, and storage facilities, and in safes or other secure containers.

- j. I know that drug traffickers often attempt to protect and conceal drug proceeds through money laundering, including but not limited to domestic and international banks, securities brokers, service professionals, such as attorneys and accountants, casinos, real estate, shell corporations, business fronts, and otherwise legitimate businesses which generate large quantities of currency. I know that it is common for drug traffickers to obtain, secrete, transfer, conceal, or spend drug proceeds, such as currency, financial instruments, precious metals, gemstones, jewelry, books, real estate, and vehicles. I know that it is also common for drug traffickers to maintain documents and records of these drug proceeds, such as bank records, passbooks, money drafts, transaction records, letters of credit, money orders, bank drafts, titles, ownership documents, cashier's checks, bank checks, safe deposit box keys, money wrappers, and other documents relating to the purchase of financial instruments or the transfer of funds. I know that drug traffickers often purchase or title assets in fictitious names, aliases, or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are titled or purchased by nominees, the drug traffickers actually own, use, and exercise dominion and control over these assets. The aforementioned books, records, receipts, notes, ledgers, and other documents are often maintained where the traffickers have ready access. These may be stored in hard copy or soft copy on paper, computers, cellular devices, and other electronic media or electronic storage devices.
- k. Digital currency, also known as crypto-currency, is generally defined as an electronic-sourced unit of value, which can substitute for fiat currency. Digital currency exists entirely on the Internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network.
- l. Bitcoin is one type of digital currency. Bitcoin payments are recorded in a public ledger maintained by peer-to-peer verification and is, therefore, not maintained by a single administrator or entity. Individuals can acquire bitcoins either by "mining" or by purchasing Bitcoins from other individuals. An individual can "mine" for Bitcoins by allowing his computing power to verify and record the bitcoin payments into a public ledger. Individuals are rewarded for this by receiving newly-created

Bitcoins. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be performed on any type of computer.

- m. Bitcoins are stored on digital “wallets.” A digital wallet essentially stores the access code that allows an individual to conduct bitcoin transactions on the public ledger. To access bitcoins on the public ledger, an individual must use a public address (or “public key”) and a private address (or “private key”). The public address is similar to an account number while the private key is similar to an account password. Even though the public addresses of transactors are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, an investigator could determine what transactions were conducted by that individual or entity. Bitcoin transactions are, therefore, described as “pseudonymous,” or partially anonymous.
- n. A Binance account has multiple “wallets,” sub-accounts, or sub-wallets for holding different currency (e.g., U.S. dollars, Bitcoin, Dogecoin, TetherUS, Bitcoin Cash, Bitcoin Gold), but all of the sub-wallets are within one account. The funds can be readily moved from one currency to another currency within the same account. The value of the cryptocurrency relative to the U.S. dollar is constantly changing so the exact value is unknown until the funds are transferred out. Many Bitcoin companies allow the account holder to control the “key” for each wallet and that “key” is needed to transfer or remove funds. However, Binance controls the “key” to each of the wallets on its platform.
- o. Drug traffickers often use enhanced cryptocurrency, such as Bitcoin, to protect their identities, launder money, and conceal drug proceeds, because of the anonymity provided by cryptocurrency. Bitcoin is a decentralized digital currency without a central bank or single administrator. Payments are sent from user-to-user on the peer-to-peer bitcoin network without the need for intermediaries. These services add layers of anonymity to financial transactions to evade law enforcement.
- p. I know that drug traffickers often maintain large amounts of currency, including funds in readily accessible financial accounts, to finance their ongoing drug business. I know that those involved in drug trafficking or money laundering often keep records of their transactions. Because drug trafficking generates large sums of cash, drug traffickers often keep detailed records about the distribution of narcotics and the laundering of proceeds. I also know that drug trafficking and money laundering activities require the cooperation, association, and communication between and among a number

of people. As a result, people who traffic in narcotics or launder money for such organizations possess documents that identify other members of their organization, such as telephone books, address books, handwritten notations, telephone bills, and documents containing lists of names and addresses of criminal associates. Such records also provide information about the identities of co-conspirators who launder money and traffick drugs. I also know that drug traffickers commonly maintain addresses or telephone numbers which reflect names, addresses, or telephone numbers of their drug trafficking and money laundering associates in hard copy and soft copy on papers, books, computers, cellular devices, and other electronic media or electronic storage devices.

- q. I know that drug traffickers often use electronic devices, such as telephones, cellular devices, computers, and currency counting machines to generate, transfer, count, record, or store the information described above and conduct drug trafficking and money laundering. I am familiar with computers, cellular devices, pagers, and other electronic media or electronic storage devices and their uses by drug traffickers to communicate with suppliers, customers, co-conspirators, and fellow traffickers. These devices often contain evidence of illegal activities in the form of communication records, voicemail, email, text messages, video and audio clips, location information, business records, and transaction records. I know drug traffickers take, store, preserve, or maintain photographs or videos of themselves, their associates, their property, their drugs, and their drug proceeds. These traffickers usually maintain these photographs or videos on computers, cellular devices, and other electronic media or electronic storage devices. Based upon my training and experience, I know that computer hardware and software can be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime; and (2) the objects may have been used to collect and store information about crimes. I know the following information can be retrieved to show evidence of use of a computer or smartphone to further the drug trade: system components, input devices, output devices, data storage devices, data transmission devices, and network devices and any data contained within such systems; computer media and any data contained within such media; operating system software, application or access program disks, manuals, books, brochures, or notes, computer access codes, user names, log files, configuration files, passwords, screen names, email addresses, IP addresses, and SIM cards.
- r. I have participated in numerous drug trafficking investigations involving the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these devices. This has led to evidence of the crimes under investigation and

corroborated information already known or suspected by law enforcement. I have regularly used electronic evidence to find proof relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of suspects and conspirators; and

- s. I have also participated in the execution of numerous premises search warrants and arrests, where controlled substances, firearms, drug paraphernalia, drug proceeds, electronic devices, and records relating drug trafficking and drug proceeds were seized.

4. This affidavit is based upon my personal knowledge and upon information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom I have had regular contact regarding this investigation.

5. Because this affidavit is submitted for the limited purpose of securing authorization for the warrant, I have not included each fact known to me concerning this investigation. I have set forth only the facts that I believe are essential to establish probable cause for the requested warrant.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 829(e), 841(a)(1), 841(h), 843(c)(2)(A), and 846 have been committed by NITIN MISHRA, LARRY BATTENFELD, and others. There is also probable cause to search the information described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. Based on the investigation described below, case agents have identified Indian national NITIN MISHRA residing in Lucknow, India, who was coordinating bulk drug parcels to be shipped into the United States to LARRY BATTENFELD and others to be broken down and reshipped to customers; operating an illegal online pharmacy distributing controlled substances to the United States; and, coordinating the shipment of controlled substances already located within the United States to customers.

9. In 2015, the Milwaukee District Office of the DEA initiated an investigation into a series of related internet pharmacies, which advertised controlled and non-controlled pharmaceuticals for sale without requiring a prescription. During the course of the investigation in 2019, case agents identified a co-conspirator in Florida (hereinafter referred to as “SOI-1”) and a co-conspirator in Texas (hereinafter referred to as “SOI-2”). These two co-conspirators were working together to receive bulk shipments of controlled pharmaceuticals and reship them to customers throughout the United States. An undercover agent in the Eastern District of Wisconsin purchased controlled pharmaceuticals numerous times from SOI-1 and SOI-2 between July 2019 and August 2020. Subsequent analysis of these suspected controlled substances by the DEA laboratory identified controlled substances including heroin, methamphetamine, ketamine, tramadol, diazepam, alprazolam, and modafinil.

10. In August 2020, case agents executed federal search warrants in Florida and Texas at the residences of SOI-1 and SOI-2. Case agents seized electronic devices and documents containing evidence identifying many of the drug suppliers and customers and communication related to the sale of controlled substances and money laundering of drug proceeds. Case agents also seized approximately \$100,000 in drug proceeds and different types of suspected controlled pharmaceuticals. Case agents have had the opportunity to interview SOI-1 and SOI-2 multiple times about the various drug suppliers and the circumstances around communication with the suppliers and drug payments to the suppliers. SOI-1 and SOI-2 identified multiple drug suppliers, email accounts, Bitcoin accounts, and WhatsApp accounts used by their drug suppliers to conduct drug transactions.

11. SOI-1 identified an online pharmacy www.pill2days.com ("PILL2DAYS"), from which SOI-1 had purchased Xanax (a Schedule IV controlled substance) and suspected Adderall (a Schedule II controlled substance) in the summer of 2020. SOI-1 communicated with the website representative via email. Case agents later reviewed these emails and observed the discussions about controlled substances being shipped from overseas to the United States, controlled substances being shipped domestically from re-shippers located in the United States, prices, a drug photograph, and quantities. SOI-2 was responsible for sending the drug payments, so SOI-2 communicated with a website representative via telephone at a phone number known to be used by the online pharmacy PILL2DAYS.

12. SOI-1 and SOI-2 were told by PILL2DAYS representatives that they ship pharmaceuticals from overseas to U.S. customers at the advertised prices on the website. At a significantly higher price, U.S. customers can receive the drug parcels from domestic re-shippers

they have established. SOI-1 stated he was aware of re-shippers in Arizona and Florida. In August 2020, case agents were able to intercept and seize a parcel from PILL2DAYS to SOI-2, which was supposed to contain 360 tablets of Adderall. This parcel was shipped by a re-shipper in Vermont. These tablets were sent to the DEA laboratory, and found to contain 364 tablets of modafinil (a Schedule IV controlled substance). Case agents later reviewed financial records and found that SOI-1 and SOI-2 sent payment for the Xanax and Adderall purchases to bank accounts being used by the drug trafficking organization to process customer payments.

13. Case agents reviewed the PILL2DAYS online pharmacy website www.pill2days.com. This website offers the following controlled substances for sale:

- Adderall – a Schedule II controlled substance
- Phentermine – a Schedule IV controlled substance
- Diazepam – a Schedule IV controlled substance
- Ativan – a Schedule IV controlled substance
- Klonopin – a Schedule IV controlled substance
- Xanax – a Schedule IV controlled substance
- Ambien – a Schedule IV controlled substance
- Soma (carisoprodol) – a Schedule IV controlled substance
- Tramadol - a Schedule IV controlled substance.

14. In December 2020, case agents began conducting multiple undercover purchases from PILL2DAYS. To date, case agents have purchased drugs, including but not limited to tramadol, tapentadol, purported oxycodone, purported hydrocodone, purported Adderall, codeine, and Xanax (alprazolam). This drug trafficking organization has a regular supply providing

counterfeit oxycodone (containing fentanyl and p-fluorofentanyl) and counterfeit Adderall (containing methamphetamine, fentanyl and p-fluorofentanyl).

15. While conducting undercover buys from PILL2DAYS, case agents received a drug parcel and letter, via USPS, from a Vermont domestic shipper on behalf of NITIN MISHRA, using the alias Ricky Sequierra. This letter solicited the undercover to buy drugs directly from MISHRA in the future, instead of PILL2DAYS, who MISHRA supplies.

16. On February 8, 2021, case agents conducted an undercover purchase from PILL2DAYS, via the telephone number (202) 753-9072, which is published on the website. Case agents purchased 180 tablets of tapentadol 100mg (a Schedule II controlled substance) and 180 tablets of purported hydrocodone 10mg (a Schedule II controlled substance). In connection with the purchase, case agents were directed via text message to conduct a bank transfer by Zelle, to a bank account used by the drug trafficking organization to accept drug payments. Case agents received the shipment of 180 purported hydrocodone 10mg tablets from the Vermont shipper working for MISHRA. Case agents received the shipment of 180 tablets of tapentadol 100mg from a different domestic shipper also supplying PILL2DAYS. In addition to the purported hydrocodone parcel from MISHRA's Vermont shipper, case agents also received a separate letter from MISHRA's shipper containing a sample of two of the same type of tablets which the letter referred to as "2 pain killers." This letter solicited the undercover to make drug purchases directly from MISHRA in the future instead of from PILL2DAYS. This letter identified a phone number, email address saferxforyou@gamil.com, and MISHRA's alias of Ricky Sequierra. The medications were sent to the DEA laboratory in Chicago, and the analysis confirmed the presence of tapentadol (a Schedule II controlled substance) in the tapentadol parcel. The 180 tablets of

purported hydrocodone and the two sample “pain killers” all contained tramadol (a Schedule IV controlled substance).

17. On February 17, 2021, the undercover communicated with MISHRA at the phone number and then email address included on the letter sent by MISHRA’s Vermont drug shipper. The undercover explained he was a drug re-shipper. MISHRA said he can supply the undercover with up to 25,000 tablets at one time. MISHRA stated he had just spent \$30,000 for 25,000 Xanax tablets and has two people in the United States working for him. MISHRA stated that he had the following available drugs for sale:

- Xanax (a Schedule IV controlled substance)
- Valium (a Schedule IV controlled substance)
- Ambien (a Schedule IV controlled substance)
- Ativan (a Schedule IV controlled substance)
- Viagra (non-controlled but prescription drug)
- Tramadol (a Schedule IV controlled substance)
- Hydrocodone (a Schedule II controlled substance)
- Oxycontin (a Schedule II controlled substance)
- Soma (a Schedule IV controlled substance)
- Clonazepam (a Schedule IV controlled substance)
- Tapentadol (a Schedule II controlled substance).

18. On February 22, 2021, the Honorable Stephen C. Dries, United States Magistrate Judge, issued a warrant for records and information from Google for Google account saferxforyou@gmail.com, an account used by MISHRA.

19. Case agents reviewed records received from Google pertaining to Google account saferxforyou@gmail.com. Case agents found spreadsheets identifying customers by name and address, drugs ordered (tramadol, Xanax, Ambien, Ativan, Valium, clonazepam, Soma, tapentadol, hydrocodone, Adderall, phentermine, Cialis), quantity of pills, and tracking numbers. Some of the orders went back as far as 2015. The IP addresses used to create and access this Google account are all located in India, which is where MISHRA resides. In addition, the person in India who created the email account recorded their date of birth as “July 5, 1991”, while case agents know MISHRA’s date of birth is June 5, 1991. Case agents believe MISHRA created this account and altered his date of birth slightly.

20. Case agents reviewed the email content for the email account saferxforyou@gmail.com. Several incoming emails from the dating website “OkCupid” were observed, and they referred to this email account user as “Nitin.” In another email, the account user said: “My name is Nitin.” In the majority of emails, the user refers to himself as “Ricky”, which MISHRA later told the undercover is his alias. The emails contained extensive evidence of distribution of various types of controlled pharmaceuticals. These emails included the sale of controlled substances, directing the payments for controlled substances, and tracking numbers for sent drug parcels. The account user directed many drug purchasers to send payment, via Western union, to Ashish Kumar Mishra in India. Case agents believe this is a family member of NITIN MISHRA. Emails also exist identifying the two Vermont re-shippers working for MISHRA by name.

21. On May 5, 2021, case agents conducted an undercover purchase from MISHRA, via WhatsApp, at a phone number provided by MISHRA. Case agents purchased 450 tablets of

tramadol 100mg (a Schedule IV controlled substance). MISHRA informed the undercover that his Vermont shipper had just received 40,000 tramadol tablets a week before, and he was already down to 15,000 tablets remaining in stock. MISHRA sent the undercover a video of the Vermont shipper opening the bulk drug parcel containing MISHRA's 40,000 tramadol tablets in blister packs indicating they were manufactured in India. In connection with the purchase, case agents were directed via text message to conduct a bank transfer by Zelle to a bank account associated with MISHRA's Vermont shipper. MISHRA called the undercover. Before MISHRA would have the drug parcel shipped, he asked the undercover if he was a "cop" and said he was not in the United States. Case agents received the shipment of approximately 450 tramadol 100mg tablets in the same blister packs shown in the video sent by MISHRA. This medication was sent to the DEA laboratory in Chicago, and the 450 tablets were found to contain tramadol. During this drug purchase, MISHRA also offered the undercover Xanax 1mg tablets. MISHRA said 20,000 Xanax tablets would arrive this week, and 8,000 tablets were already preordered by a customer.

22. On May 17, 2021, case agents conducted an undercover purchase from MISHRA, via WhatsApp, at a phone number provided by MISHRA. Case agents purchased 180 tablets of purported oxycodone 30mg (a Schedule II controlled substance) and 70 tablets of tapentadol 100mg (a Schedule II controlled substance). In connection with the purchase, case agents were directed via text message to conduct a bank transfer by Zelle to a bank account associated with MISHRA's Vermont shipper. The purported oxycodone parcel was incorrectly addressed to the undercover. As a result, it was returned to sender, but case agents seized the parcel. Due to MISHRA believing the undercover did not receive the first parcel, he had a second oxycodone parcel shipped to the undercover, resulting in two parcels containing purported oxycodone. During

the placement of this order, MISHRA informed the undercover that MISHRA had 5,000 to 6,000 tramadol tablets and 1,800 oxycodone tablets in stock and also had 10,000 Xanax tablets and 16,000 hydrocodone tablets in transit. Case agents received the shipment of 70 tapentadol 100mg tablets from MISHRA's Vermont shipper. Both parcels containing purported oxycodone parcels were shipped from a shipper in California. The medications were sent to the DEA laboratory in Chicago. One purported oxycodone parcel contained 180 counterfeit pills which tested positive for the presence of tramadol (a Schedule IV controlled substance) and alprazolam (a Schedule IV controlled substance). The second purported oxycodone parcel contained 188 counterfeit pills which tested positive for the presence of tramadol (a Schedule IV controlled substance). The tapentadol parcel contained 70 tablets in blister packs indicating it was manufactured in India. This tapentadol medication tested positive for the presence of tapentadol (a Schedule II controlled substance).

23. On May 26, 2021, MISHRA messaged the undercover via WhatsApp. MISHRA informed the undercover that MISHRA had two parcels of 30,000 tablets each of zolpidem (a Schedule IV controlled substance) in transit to his shipper. MISHRA said he bought the 60,000 zolpidem tablets from an associate located within the U.S. who had 90,000 tablets. MISHRA said this same associate offered to sell MISHRA 150,000 tramadol tablets for \$300,000.

24. On June 29, 2021, case agents executed federal search warrants related to two of MISHRA's co-conspirators in Vermont who were receiving the bulk drug parcels and reshipping them on behalf of MISHRA. Case agents seized approximately 15,000 zolpidem tablets from one Vermont residence and approximately 15,000 tablets of various Schedule II and IV controlled pharmaceuticals from the other Vermont residence. The federal prosecution of these Vermont co-

conspirators is occurring in the District of Vermont. During the search of one of the residences, case agents noted that target's cell phone received several incoming WhatsApp phone calls. While looking at the screen of the target's cell phone, case agents observed the incoming phone calls were from a person saved in the phone as "Nitn." Case agents believe these incoming calls were from NITIN MISHRA.

25. On June 29, 2021 and the days after, MISHRA informed the undercover, via WhatsApp, that his drug shippers in Vermont were arrested, and all of the drugs were seized by law enforcement.

26. On September 8, 2021, MISHRA informed the undercover that an associate of his has oxycodone 30mg and Adderall 30mg in stock. MISHRA sent the undercover photographs of these pills packaged in unique Ziploc bags on USPS shipping envelopes displaying partial return address/name. Case agents recognized the unique packaging and return address/name from a shipper in Texas, who is also shipping for PILL2DAYS. The counterfeit oxycodone purchased from this shipper was found to contain fentanyl, and the counterfeit Adderall purchased from this shipper was found to contain methamphetamine.

27. On October 19, 2021, case agents conducted an undercover purchase from MISHRA, via WhatsApp, at a phone number provided by MISHRA. Case agents purchased 270 tablets of purported oxycodone 30mg (a Schedule II controlled substance), which MISHRA said belongs to his associate. Case agents know that associate is known to supply counterfeit oxycodone tablets containing fentanyl. Case agents also purchased 340 tablets of tramadol 100mg (a Schedule IV controlled substance). MISHRA stated the tramadol tablets were being shipped by a California shipper, later identified as LARRY BATTENFELD, who MISHRA asked to take over shipping

for the arrested Vermont shippers. MISHRA stated this California shipper is shipping up to approximately 10,000 tablets of primarily tramadol per month on behalf of MISHRA. In connection with the purchase, case agents were directed, via WhatsApp message, to send payment in the form of Bitcoin directly to MISHRA's personal Binance account at Bitcoin address 1BioM6h96YmHk5KHqspwsKyg1KeczpsFhw. The undercover transferred 0.03276677 BTC (valued at \$2,075.20 USD). Case agents received the shipment of approximately 340 tramadol 100mg tablets from MISHRA's California shipper, packaged in blister packs indicating the medication was manufactured in India. Case agents received the shipment of approximately 270 purported oxycodone 30mg tablets from a shipper in Pennsylvania who is believed to be supplied by the same counterfeit oxycodone and Adderall source of supply. These medications were sent to the DEA laboratory in Chicago for analysis. The purported oxycodone consisted of 277 tablets containing only acetaminophen, and the tramadol consisted of 340 tablets containing tramadol.

28. The return address of the tramadol parcel shipped to case agents by LARRY BATTENFELD listed the sender as CNS with a return address of P.O. Box 621, Cedar Ridge, CA 95924-0621.

29. Case agents reviewed the USPS Post Office Box account holder details for return address "P.O. Box 621." The account holder details are as follows:

- a. Name: LARRY BATTENFELD
- b. California Driver's License: A3991799
- c. California DOT check lists to LARRY BATTENFELD
- d. Email: **lktechnologies@comcast.net**
- e. Address: 12936 Colfax Highway, Grass Valley, California 95945

f. Phone: (530) 277-0122.

30. On October 20, 2021, case agents received records from the crypto-currency exchange Binance, pursuant to a DEA administrative subpoena. These records identified the account holder of the Binance account case agents sent the drug payment to on October 19, 2021, which MISHRA said was his personal account. The records included IP addresses used to access this account, and the IP addresses are located in Lucknow, India. The Binance account records identify the account holder as the following:

- a. Name: NITIN MISHRA
- b. Binance account User ID #219978945
- c. DOB: June 5, 1991
- d. Indian Identification: ID #CKCPM7998D
- e. Email: aryalenn@gmail.com
- f. Phone: +91-9971501773 (India).

31. MISHRA communicated with the undercover regarding the Bitcoin payment, and MISHRA acknowledged receiving the payment shortly after the undercover sent payment. MISHRA also explained how he used a third party to transfer the Bitcoin into cash, so MISHRA could provide a portion of the funds to the associate who controls the purported oxycodone which was purchased. MISHRA stated he did not want to exchange the Bitcoin into fiat currency in his own bank account because tax reporting agencies would question the source of funds. MISHRA explained he was able to keep the other portion of the payment because MISHRA is the owner of the tramadol stock in California. The Binance records show the undercover's payment went directly into this Binance account User ID #219978945, held in the name of NITIN MISHRA.

The Binance records also included an image of the front and rear of MISHRA's Indian government identification card which includes his photograph. Furthermore, Binance provided a "live photo," which MISHRA was required to provide when creating this Binance account. Case agents know that Binance requires this "live photo" to verify the person creating the account is truly the person depicted on the identification card.

32. On October 27, 2021, the Honorable William E. Duffin, United States Magistrate Judge of the Eastern District of Wisconsin, issued a pen register and trap-and-trace order on the WhatsApp accounts associated with call numbers (435) 518-7269 and +91-9971501773, which are both used by NITIN MISHRA. Case agents found that between November 1, 2021 and December 25, 2021, MISHRA, using (435) 518-7269, communicated with phone number (530) 277-0122, approximately 748 times. According to USPS Post Office Box and Stamps.com records, phone number (530) 277-0122 belongs to LARRY BATTENFELD. BATTENFELD routinely sent messages to MISHRA while BATTENFELD was connected to IP address 71.197.72.194. Records were acquired from Comcast Communications, pursuant to a DEA administrative subpoena, which identified the Comcast Communications account holder details related to this IP address as the following:

- a. Name: William Battenfeld
- b. Address: 12936 Colfax Highway, Grass Valley, California 95945
- c. Phone: (530) 913-7388.

33. On November 5, 2021 and November 8, 2021, the undercover recorded three WhatsApp video calls between the undercover and MISHRA discussing drug trafficking. MISHRA has repeatedly tried soliciting the undercover to invest \$50,000 in a joint venture so

MISHRA can use that money to purchase bulk drug parcels. These drug parcels would be shipped to the undercover in Milwaukee for the undercover to reportedly ship to customers who MISHRA would identify. The undercover clearly saw MISHRA's face during these video calls and was able to identify him as the same person depicted in MISHRA's Indian identification card, the Binance "live photo," a photograph MISHRA sent the undercover of himself at the gym, a Facebook profile photograph for "Nitin Mishra," and a WhatsApp profile photograph for a number MISHRA previously used to communicate with the undercover.

34. On November 18, 2021, case agents conducted an undercover purchase from MISHRA, via WhatsApp, at a phone number provided by MISHRA. MISHRA sent the undercover a video of his domestic shipper (believed to be LARRY BATTENFELD) opening a bulk parcel of 6,000 tramadol tablets that MISHRA had shipped to this shipper. The video shows the thousands of tramadol tablets in blister packs and how the drugs were concealed. The undercover was also able to hear the voice of the male subject (believed to be LARRY BATTENFELD) as he opened the parcel, and the undercover could see this person was wearing a wedding band and has a distinct tattoo on the same hand as the wedding band. Case agents purchased 180 tablets of purported oxycodone 30mg (a Schedule II controlled substance) and 270 tablets of purported Adderall 30mg (a Schedule II controlled substance). MISHRA informed the undercover that these controlled substances were being shipped by the same source of supply that case agents know previously shipped counterfeit oxycodone (fentanyl) and counterfeit Adderall (methamphetamine) for PILL2DAYS. The undercover asked MISHRA to also ship the undercover tramadol 100mg from his California shipper with any remaining funds. MISHRA had his California shipper send 80 tramadol 100mg tablets (a Schedule IV controlled substance) and 20

Ambien tablets (a Schedule IV controlled substance) to the undercover. In connection with the purchase, case agents were directed, via WhatsApp message, to send payment in the form of Bitcoin directly to MISHRA's same personal Binance account at Bitcoin address 1BioM6h96YMhk5KHqspwsKyg1KeczpsFhw. The undercover transferred 0.03498791 BTC (valued at \$2,010.48 USD). Case agents received the shipment of 80 tramadol 100mg tablets and 20 tablets of Ambien tablets from MISHRA's California shipper LARRY BATTENFELD packaged in blister packs indicating the medication was manufactured in India. Case agents received the shipment of 180 purported oxycodone 30mg tablets and 270 purported Adderall 30mg tablets. These medications were sent to the DEA laboratory in Chicago for analysis. The purported oxycodone tablets were tested and contain a mixture of fentanyl, fluorofentanyl, and acetaminophen with a 19.5 gram net weight. The purported Adderall tablets were tested and contain a mixture of fentanyl and acetaminophen with a 91.3 gram net weight. Case agents conducted a field test of the tramadol and zolpidem tablets utilizing a TruNarc device. The test results show the presence of tramadol and zolpidem.

35. Case agents were able to trace the undercover's drug payment and review Binance records to confirm the payment was made directly to MISHRA's same Binance Account User ID #219978945, held in the name of NITIN MISHRA.

36. The parcel containing the tramadol and Ambien tablets originally arrived at the undercover mailbox, but then it was erroneously returned to sender by the U.S. Postal Service. The original parcel displayed LARRY BATTENFELD's return address—P.O. Box 621, Cedar Ridge, California. MISHRA informed the undercover that his California shipper (known to be LARRY BATTENFELD) received the returned drug parcel at the return address and would reship

the drugs. Per U.S. Postal Service records, LARRY BATTENFELD listed only himself as the person authorized to have access to P.O. Box 621. The reshipped parcel eventually received by case agents displayed the following return address:

- a. LARRY BATTENFELD
- b. 12700 Colfax Highway, Unit 621 (physical address for P.O. Box 621)
- c. Cedar Ridge, CA 95924-2027.

37. On November 18, 2021, MISHRA informed the undercover that MISHRA's sister helped him create an online pharmacy website www.buyyourmed.com. MISHRA stated he is also using another company to direct customers to his website. MISHRA stated he will handle all the customer service tasks himself. Based on prior experience, this would include taking orders, accepting payments, and coordinating drug shipments. Case agents reviewed this website which listed the customer service contact details as phone number (202) 858-4068, email address saferrxforu@gmail.com, and location as California. These are the same contact details that were included in the original letter mailed to the undercover when MISHRA was attempting to solicit business away from PILL2DAYS. MISHRA said he was the one who personally typed the letter and had the Vermont shipper disseminate the letter to customers. Case agents know that LARRY BATTENFELD is located in California. A review of the www.buyyourmed.com website revealed the following medications for sale: Ativan (a Schedule IV controlled substance); Valium (a Schedule IV controlled substance); Adderall (a Schedule II controlled substance); hydrocodone (a Schedule II controlled substance); oxycodone (a Schedule II controlled substance); tramadol (a Schedule IV controlled substance); tapentadol (Nucynta) (a Schedule II controlled substance); Cialis (a non-controlled prescription drug); Viagra (a non-controlled prescription drug); Xanax

(alprazolam) (a Schedule IV controlled substance); Klonopin (clonazepam) (a Schedule IV controlled substance); Ambien (zolpidem) (a Schedule IV controlled substance); and Soma (carisoprodol) (a Schedule IV controlled substance).

38. Case agents reviewed the images and description of the drugs available for sale from the website. Case agents recognized the images of Adderall and oxycodone as the same images MISHRA previously sent to the undercover. Case agents know that these oxycodone and Adderall tablets are counterfeit, containing fentanyl and Adderall, because case agents have purchased them several times from the same shipper through PILL2DAYS. Case agents also noted the same counterfeit hydrocodone 10mg tablets offered by the same shipper previously contained fentanyl.

39. On February 24, 2022, case agents conducted an undercover purchase from MISHRA, via WhatsApp, at a phone number provided by MISHRA. Case agents purchased 180 tablets of purported Adderall 30mg (a Schedule II controlled substance) and 540 tablets of Ambien (a Schedule IV controlled substance). MISHRA stated the Ambien would be shipped by his domestic shipper, known to case agents as LARRY BATTENFELD. In connection with the purchase, case agents were directed, via WhatsApp message, to send payment in the form of Bitcoin directly to MISHRA's same personal Binance account at Bitcoin address 1BioM6h96YMHk5KHqspwsKyg1KeczpsFhw. The undercover transferred 0.09518811 BTC (valued at \$3,538.24 USD). Case agents received the shipment of 181 Adderall 30mg tablets and 520 tablets of Ambien 10mg tablets from LARRY BATTENFELD. The return address displayed on the Ambien parcel is CNS P.O. Box 621, Cedar Ridge, CA 95924-0621, which is rented by LARRY BATTENFELD and linked to email address **lktechnologies@comcast.net**. These

medications were sent to the DEA laboratory in Chicago for analysis. The purported Adderall tablets were tested and contain a mixture of fentanyl, fluorofentanyl, caffeine, and acetaminophen with a net weight of 57.6 grams. The Ambien tablets were tested and contain zolpidem.

40. Case agents were able to trace the undercover's drug payment and review Binance records to confirm the payment was made directly to MISHRA's same Binance Account User ID #219978945, held in the name of NITIN MISHRA.

41. On April 14, 2022, case agents conducted an undercover purchase from MISHRA, via WhatsApp, at a phone number provided by MISHRA. Case agents purchased 230 tablets of Ambien (a Schedule IV controlled substance). MISHRA stated the Ambien would be shipped by his domestic shipper, known to case agents as LARRY BATTENFELD. In connection with the purchase, case agents were directed, via WhatsApp message, to send payment to a Zelle account linked to email address **lktechnologies@comcast.net**. Case agents received the shipment of 230 tablets of Ambien 10mg from LARRY BATTENFELD. The return address displayed on the Ambien parcel is CNS P.O. Box 621, Cedar Ridge, CA 95924-0621, which is rented by LARRY BATTENFELD and linked to email address **lktechnologies@comcast.net**. The medication was sent to the DEA laboratory in Chicago for analysis, and the results are pending.

42. During this undercover drug buy, MISHRA asked if an undercover of the U.S. Food and Drug Administration (FDA) could assist in transferring the drug payment that was just made from BATTENFELD to MISHRA. BATTENFELD was having difficulty transferring the funds directly to MISHRA without paying high fees. The DEA undercover previously introduced the FDA undercover to MISHRA. At MISHRA's request, BATTENFELD subsequently transferred the drug proceeds on April 19, 2022 to the FDA undercover via Zelle from an account in the name

of “Expert Stove & Fireplace.” Case agents know this Zelle account is registered to BATTENFELD’s email account **lktechnologies@comcast.net**. The FDA undercover then transferred the drug proceeds to an account as directed by MISHRA with ICICI Bank in Lucknow, India and the beneficiary listed as Quantum Solutions.

43. Case agents learned that all drug parcels shipped to the DEA undercover from LARRY BATTENFELD had postage paid by the same Stamps.com account. Case agents received Stamps.com records via DEA administrative subpoena. These records provided a list of IP addresses used to access the Stamps.com account. As of March 8, 2022, this account had been used to ship 586 suspected drug parcels. The Stamps.com account holder details are as follows:

- a. Name: LARRY BATTENFELD
- b. Billing/Mailing Address: P.O. Box 621, Cedar Ridge, CA 95924
- c. Physical Address: 12936 Colfax Highway, Grass Valley, CA 95945
- d. Email: **lktechnologies@comcast.net**
- e. Phone: (530) 277-0122.

44. Case agents received records from Comcast, pursuant to a DEA administrative subpoena. These records are related to Comcast IP address 71.197.72.194 which was consistently used to access the Stamps.com account to create shipping labels. These Comcast records identify the account holder and the location of the customer as the following:

- a. Name: William Battenfeld
- b. Address: 12936 Colfax Highway, Grass Valley, CA 95945
- c. Phone: (530) 913-7388.

45. Case agents received records from Comcast, pursuant to a DEA administrative subpoena, for the email address **lktechnologies@comcast.net**. These Comcast records identify the email subscriber as the following:

- Name: LARRY BATTENFELD
- Address: 13692 Highland Drive, Grass Valley, CA 95945.

46. On June 3, 2022, case agents received records from Zelle, pursuant to a grand jury subpoena. These Zelle records relate to the account to which the DEA undercover sent a drug payment, which is linked to email address **lktechnologies@comcast.net**. The records show this Zelle account is linked to multiple email addresses including **lktechnologies@comcast.net**. LARRY BATTENFELD and William Battenfeld are both affiliated with the Zelle account.

47. Case agents reviewed records of a Zelle account listing to MISHRA's prior drug shipper in Vermont. These records were acquired pursuant to a DEA administrative subpoena. These records revealed that LARRY BATTENFELD's Zelle account linked to email address **lktechnologies@comcast.net** sent funds to the Vermont drug shipper on April 30, 2021.

48. On August 23, 2022, case agents conducted a records checks of LARRY BATTENFELD through the California Department of Transportation (DOT). The California DOT records revealed that BATTENFELD listed his P.O. Box address of 12700 Colfax Highway, Unit 621, Cedar Ridge, California 95924 with the DOT. The distance between this post office containing P.O. Box 621 and 12936 Colfax Highway, Grass Valley, California, 95945 is 0.2 miles.

49. On August 26, 2022, case agents conducted an undercover purchase from MISHRA, via WhatsApp, at a phone number provided by MISHRA. MISHRA stated his same domestic shipper (LARRY BATTENFELD) received bulk quantities of zolpidem and tapentadol.

MISHRA was referring to tapentadol when he said this shipper received 40,000 tablets on behalf of MISHRA. Case agents purchased 1,000 tablets of tapentadol 100mg (a Schedule II controlled substance). In connection with the purchase, case agents were directed, via WhatsApp message, to send payment in the form of Bitcoin directly to MISHRA's same personal Binance account at Bitcoin address 1BioM6h96YMhk5KHqspwsKyg1KeczpsFhw. The undercover transferred 0.14990662 BTC (valued at \$3,100.47 USD). MISHRA requested the undercover place another order in the near future and send the payment directly to the domestic shipper LARRY BATTENFELD, via Zelle, because MISHRA owes the shipper funds. MISHRA stated he pays this shipper a percentage of drug payments when the shipper receives and transfers it overseas to MISHRA. Case agents received the shipment of 1,000 tapentadol 100mg tablets from MISHRA's California shipper LARRY BATTENFELD packaged in manufacturer's boxes and blister packs indicating the medication was tapentadol 100mg (a Schedule II controlled substance) manufactured in India. The drug parcel was shipped from the post office located at 12700 Colfax Highway, Cedar Ridge, California which is the post office in which BATTENFELD's P.O. Box is located and is located only 0.2 miles from BATTENFELD's residence at 12936 Colfax Highway, Grass Valley, California 95945. This medication was sent to the DEA laboratory in Chicago for analysis, and the results are pending.

50. The return address listed on the parcel of 1,000 tapentadol tablets was as follows:
 - a. CNS
 - b. P.O. Box 621
 - c. Cedar Ridge, CA 95924-0621.

51. Case agents were able to trace the undercover's drug payment and review Binance records to confirm the payment was made directly to MISHRA's same Binance Account User ID #219978945, held in the name of NITIN MISHRA.

52. On August 27, 2022, case agents reviewed images of multiple parcels received at LARRY BATTENFELD's P.O. Box 621, Cedar Ridge, CA 95924-0621. Case agents noted multiple parcels addressed to LARRY BATTENFELD throughout August 2022.

53. On September 7, 2022, case agents received records from Verizon pursuant to a DEA administrative subpoena for phone number (530) 277-0122, which is linked to BATTENFELD's various accounts, including his P.O. Box and Stamps.com postage account. Those records show that BATTENFELD's number was in regular communication with MISHRA. Case agents found the following Verizon subscriber details for phone number (530) 277-0122:

- a. Name: Larry "Battenfield"
- b. Address: 12700 Colfax Highway, Unit 621, Cedar Ridge, CA 95924-2027
- c. Email: **lktechnologies@comcast.net**.

54. On September 7, 2022, agents with the FDA conducted surveillance at the home of BATTENFELD located at 12936 Colfax Highway, Grass Valley, California 95945. At approximately 8:49 a.m., case agents observed a white Toyota Tundra pickup truck drive onto the roadway from the driveway of 12936 Colfax Highway, Grass Valley, California 95945. At approximately 8:52 a.m., this Toyota Tundra parked in the parking lot of the U.S. Post Office located at 12700 Colfax Highway, Grass Valley, California which is where BATTENFELD's post office box is located. Case agents first identified BATTENFELD as the driver of the Toyota Tundra, as he left the driveway of 12936 Colfax Highway, Grass Valley, California 95945 and

again when the Toyota Tundra arrived at the post office and BATTENFELD exited the vehicle. Case agents positively identified BATTENFELD from previously viewing a California driver's license photograph of BATTENFELD. Case agents watched BATTENFELD enter the post office carrying three parcels, and a short time later he returned without the parcels.

55. Case agents believe BATTENFELD left his residence located at 12936 Colfax Highway, Grass Valley, California 95945 with three drug parcels. He then drove to the nearby post office to ship the three drug parcels—the same post office from which BATTENFELD shipped the undercover's drug parcel on or about August 26, 2022.

56. On September 29, 2022, case agents received updated records through August 23, 2022 from Stamps.com, pursuant to a DEA administrative subpoena. These records are related to the Stamps.com account which BATTENFELD has been using to ship drug parcels. These records identify the most recent IP address used to access this Stamps.com account on August 23, 2022 is Comcast IP address 71.197.72.194. Case agents previously received Comcast records identifying the customer this IP address is assigned to as the following:

- Name: William Battenfeld
- Address: 12936 Colfax Highway, Grass Valley, CA 95945
- Phone: (530) 913-7388.

57. On October 12, 2022, NITIN MISHRA was arrested in Albania by Albanian and U.S. law enforcement authorities. MISHRA traveled to Albania with the intention to meet with the undercover. MISHRA wanted the undercover to transfer approximately \$70,000 in cryptocurrency to MISHRA in exchange for MISHRA coordinating the shipment of 100,000 tablets of tapentadol (a Schedule II controlled substance) to the undercover. MISHRA was arrested and

interviewed by case agents. MISHRA confessed to his role in the distribution of controlled substances within and to the United States. MISHRA said LARRY BATTENFELD is a long time tramadol customer of MISHRA. MISHRA solicited BATTENFELD to receive bulk drug parcels in the middle of 2021 and to reship the drugs to various customers throughout the United States. MISHRA said BATTENFELD has reshipped approximately 100,000 tablets of a combination of zolpidem, tramadol, tapentadol, and possibly alprazolam. According to MISHRA, BATTENFELD should have 120 tapentadol tablets remaining in his possession, and MISHRA and BATTENFELD communicated via WhatsApp and email.

58. On October 25, 2022, case agents executed a search warrant at the residence of LARRY BATTENFELD located at 12936 Colfax Highway, Grass Valley, California 95945. BATTENFELD was present, and case agents seized his cell phone and approximately 9,000 controlled pharmaceutical tablets identified by the manufacturer's blister packs as tapentadol, alprazolam, tramadol, and zolpidem. After waiving his rights, BATTENFELD provided an audio recorded statement to case agents. BATTENFELD said he began as a customer buying tramadol online for personal use. In middle of 2021, BATTENFELD was solicited by an Indian male known to BATTENFELD as "Ricky" to receive bulk drug parcels to reship to Ricky's customers. BATTENFELD provided the phone number for Ricky. Case agents know that this phone number is used by NITIN MISHRA, and "Ricky" is an alias that MISHRA uses. BATTENFELD received bulk drug parcels consisting of tramadol, tapentadol, alprazolam, and zolpidem. BATTENFELD communicated with MISHRA via WhatsApp messaging and voice calls about most matters. MISHRA would email customer drug orders, to include customer name, address, drug type, and drug quantity to BATTENFELD's email address **lktechnologies@comcast.net**. BATTENFELD

also admitted to receiving drug payments via Zelle and CashApp and creating a WhitePages account for MISHRA, which MISHRA could use to find new customers.

59. Case agents believe that SOI-1 is a reliable witness as SOI-1 has provided a statement against SOI-1's own penal interest, and information provided by SOI-1 has been independently corroborated by case agents. SOI-1's criminal history consists of misdemeanor assault and misdemeanor menacing. SOI-1 has no prior felony convictions. SOI-1 has provided information in other investigations, and that information was found to be accurate and reliable. SOI-1 is cooperating with law enforcement for potential prosecutorial and judicial consideration for his federal felony drug trafficking arrest, which remains pending.

60. Case agents believe that SOI-2 is a reliable witness as SOI-2 has provided a statement against SOI-2's own penal interest, and information provided by SOI-2 has been independently corroborated by case agents. SOI-2's criminal history consists of one prior federal felony conviction for conspiracy to commit health care fraud, mail and wire fraud, money laundering, and illegal monetary transaction, conspiracy to distribute controlled substances, and mail fraud. SOI-2 may have been arrested for forgery in the 1980s. SOI-2 has provided information in other investigations, and that information was found to be accurate and reliable. SOI-2 cooperated with law enforcement for consideration in his most recent federal felony drug trafficking case and revocation sentence for his supervised release in the prior case.

61. Case agents believe that LARRY BATTENFELD is a reliable witness as BATTENFELD has provided a statement against his own penal interest, and information provided by BATTENFELD has been independently corroborated by case agents. BATTENFELD has no

criminal history. BATTENFELD is cooperating with law enforcement for potential prosecutorial and judicial consideration for this federal felony drug trafficking arrest, which remains pending.

62. Based on the investigation described above, case agents believe that NITIN MISHRA and LARRY BATTENFELD are involved in a drug trafficking organization which imports bulk drug parcels from overseas to U.S. drug shippers working for MISHRA. These drugs then get reshipped throughout the U.S. to customers by LARRY BATTENFELD.

63. Case agents have uncovered that BATTENFELD's email address **lktechnologies@comcast.net** was used to establish accounts with Stamps.com (used to fund the shipping of drug parcels), Zelle (used to receive undercover's drug payment and send payment to Vermont drug shipper as early as April 30, 2021), and USPS P.O. Box 621 (used to receive drug parcels and as a return address on drug parcels). Case agents know that the email address used to setup these accounts will receive email alerts and other pertinent email communication. For example, when a drug payment is received by BATTENFELD via Zelle, an email alert is sent to **lktechnologies@comcast.net** with transaction details. Furthermore, case agents believe proving the person in control of the accounts with Stamps.com, Zelle, and USPS is crucial to confirming the role of LARRY BATTENFELD and others as co-conspirators. Case agents can show who is in control of these accounts by showing who is in control of the linked email address **lktechnologies@comcast.net**. Case agents know that the person in control of an email address can be identified by reviewing the email content, messaging, photographs, and other files attached to emails. Furthermore, BATTENFELD informed case agents that MISHRA would email customer drug order details to BATTENFELD at email address **lktechnologies@comcast.net**.

64. For all of the foregoing reasons, case agents are requesting a search warrant for emails containing the information set forth in Attachment B for **lktechnologies@comcast.net** for the time period of January 1, 2021 to the present.

65. Based on my training and experience, individuals who engage in interstate trafficking in controlled and non-controlled pharmaceuticals via the internet will communicate and send and receive information through electronic communication such as e-mails. Individuals engaged in criminal activity via the internet often remain anonymous by providing inaccurate or false information, but will often use e-mail accounts to conduct business and or communicate with other co-conspirators. The true identity and location of these individuals can often be found by analyzing their e-mail communication.

66. In general, an e-mail that is sent to a Comcast subscriber is stored in the subscriber's "mail box" on Comcast's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Comcast's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Comcast's servers for a certain period of time.

BACKGROUND CONCERNING E-MAIL

67. In my training and experience, I have learned that Comcast provides a variety of on-line services, including electronic mail ("email") access, to the public. Comcast allows subscribers to obtain email accounts at the domain name Comcast.net, like the email account listed in Attachment A. Subscribers obtain an account by registering with Comcast. During the registration process, Comcast asks subscribers to provide basic personal information. Therefore, the computers of Comcast are likely to contain stored electronic communications (including

retrieved and unretrieved email for Comcast subscribers) and information concerning subscribers and their use of Comcast services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

68. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

69. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the

account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

70. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

71. This application seeks a warrant to search all responsive records and information under the control of Comcast, a provider subject to the jurisdiction of this court, regardless of where Comcast has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Comcast's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

72. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or

alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

73. Based on the foregoing, I request that the Court issue the proposed search warrant.

74. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Comcast. Because the warrant will be served on Comcast, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with lktechnologies@comcast.net, that is stored at premises controlled by Comcast Communications, a company headquartered in Philadelphia, Pennsylvania.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Comcast (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A from January 1, 2021 to October 26, 2022:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 DAYS of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 21, United States Code, Sections 829(e), 841(a)(1), 841(h), 843(c)(2)(A), and 846 and occurring after January 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. The importation and distribution of controlled substances and other prescription medications.
2. Information relating to the identity of any and all individuals who operate or maintain online pharmacies that sell controlled substances and other prescription medications.
3. Records of payment made in relation to the operation and maintenance of online pharmacies that sell controlled substances and other prescription medications, including proceeds from such sales.
4. Information relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.
5. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.
6. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation.
7. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
8. The identity of the person(s) who communicated with the user ID about matters relating to importation and distribution of controlled substances and other prescription medications, including records that help reveal their whereabouts.